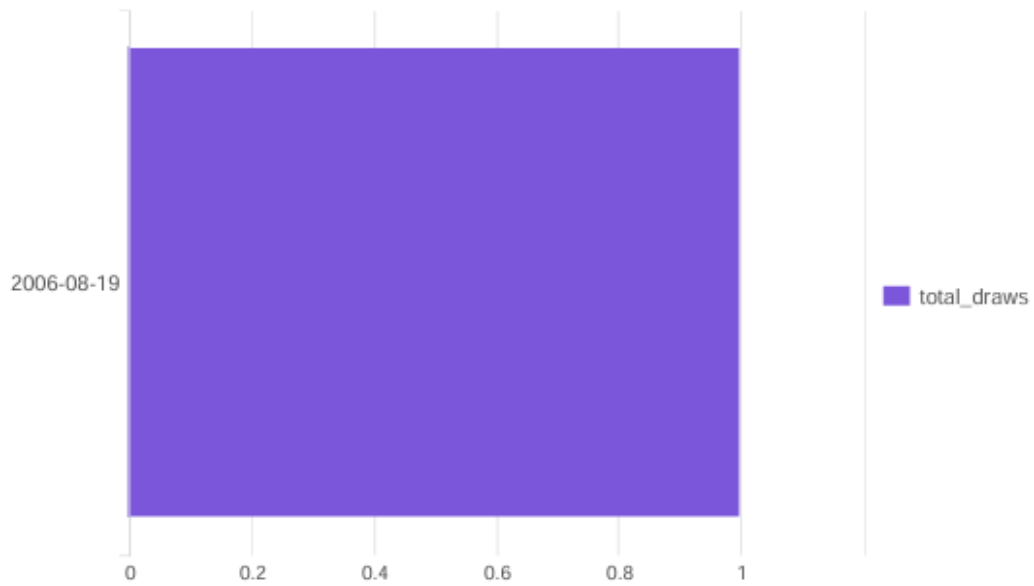
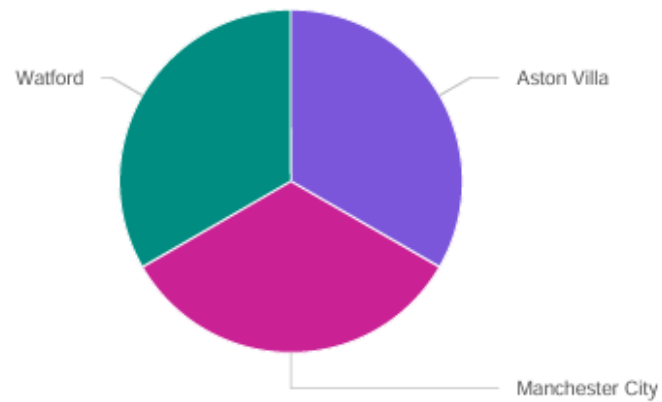


match end draw



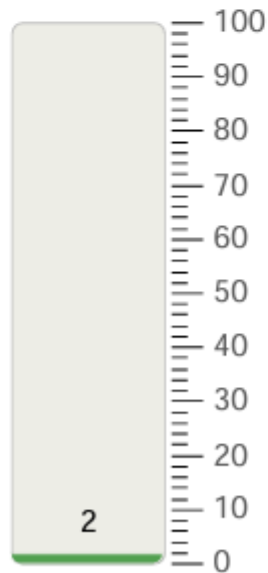
goals for teams



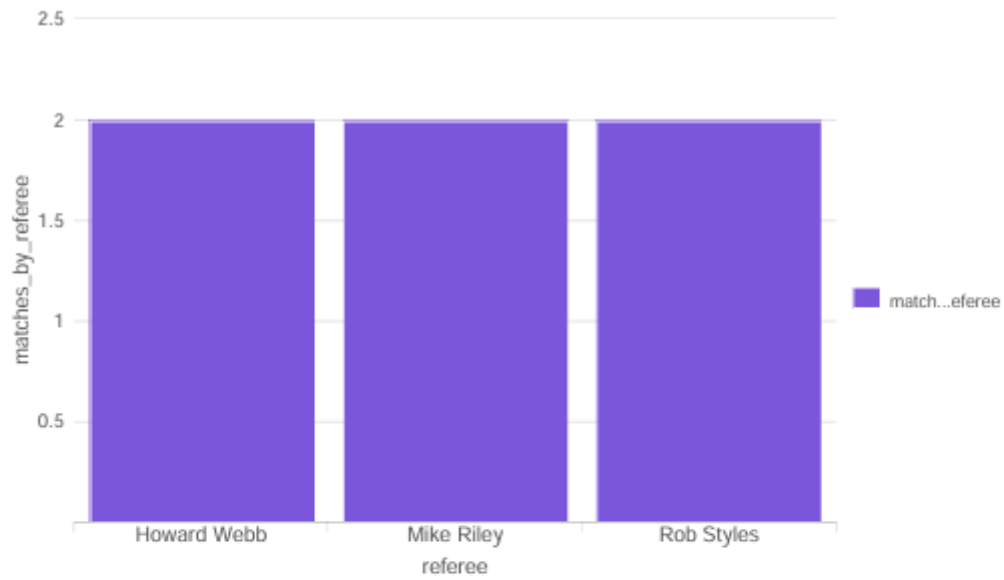
avg attendance



matches end by one goal



most referees in matches



final project football (attendance>40000)

attendance>40000

Enabled: Yes. Disable

App: search

Permissions: Private. Owned by mahmoud. Edit

Modified: Dec 24, 2024 6:51:41 AM

Alert Type: Scheduled. Weekly, Monday at 6:00. Edit

Trigger Condition: .. Number of Results is > 0. Edit

Actions:

1 Action ... Alert Run a script

Edit

The screenshot displays the Splunk Enterprise web interface. At the top, the navigation bar includes the 'splunk>enterprise' logo, an 'Apps' dropdown, and user information for 'Administrator'. Below this, a secondary navigation bar lists 'Search', 'Analytics', 'Datasets', 'Reports', 'Alerts', and 'Dashboards'. The main content area shows the configuration for an alert titled 'final project football (attendance>40000)'. The alert's search query is 'attendance>40000'. Configuration details include: 'Enabled' (Yes, with a 'Disable' link), 'App' (search), 'Permissions' (Private, Owned by mahmoud, with an 'Edit' link), 'Modified' (Dec 24, 2024 6:51:41 AM), and 'Alert Type' (Scheduled. Weekly, Monday at 6:00, with an 'Edit' link). The 'Trigger Condition' is 'Number of Results is > 0' (with an 'Edit' link), and the 'Actions' section shows '1 Action' (with a dropdown arrow) and 'Run a script' (with an 'Edit' link). An 'Edit' button is located in the top right corner of the configuration panel. At the bottom of the interface, a message states: 'There are no fired events for this alert.'

final project football (High Scoring Matches Alert)

if total > 5 football

Enabled:Yes. [Disable](#)

App:search

Permissions:Private. Owned by mahmoud. [Edit](#)

Modified:Dec 24, 2024 6:28:33 AM

Alert Type:Scheduled. Weekly, Monday at 6:00. [Edit](#)

Trigger Condition: ...Number of Results is > 0. [Edit](#)

Actions:1 Action



Add to Triggered Alerts

[Edit](#)

The screenshot shows the Splunk Enterprise web interface. At the top, there's a navigation bar with 'splunk>enterprise' and various user and system links. Below this is a secondary navigation bar with tabs for 'Search', 'Analytics', 'Datasets', 'Reports', 'Alerts', and 'Dashboards'. The main content area displays the configuration for an alert titled 'final project football (High Scoring Matches Alert)'. The alert condition is 'if total > 5 football'. The configuration details are as follows:

- Enabled:Yes. [Disable](#)
- App:search
- Permissions:Private. Owned by mahmoud. [Edit](#)
- Modified:Dec 24, 2024 6:28:33 AM
- Alert Type:Scheduled. Weekly, Monday at 6:00. [Edit](#)
- Trigger Condition: ... Number of Results is > 0. [Edit](#)
- Actions: 1 Action [Edit](#)
 - Add to Triggered Alerts

At the bottom of the alert configuration, there is a message: There are no fired events for this alert.

final project football (events for chelsea)

events for chelsea

Enabled: Yes. [Disable](#)

App:search

Permissions:Private. Owned by mahmoud. [Edit](#)

Modified:Dec 24, 2024 6:50:06 AM

Alert Type:Scheduled. Weekly, Monday at 6:00. [Edit](#)

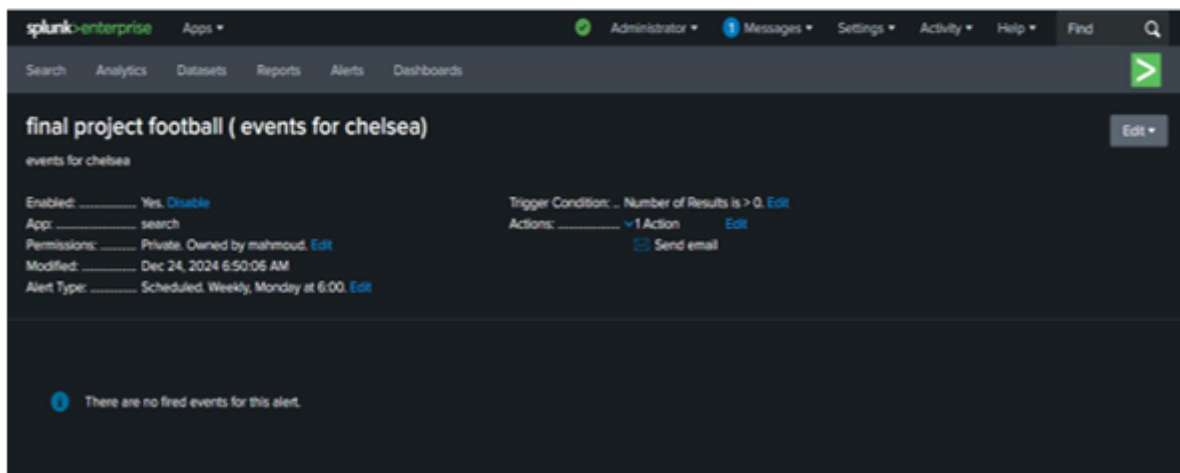
Trigger Condition:Number of Results is > 0. [Edit](#)

Actions:1 Action



Send email

[Edit](#)

A screenshot of the Splunk Enterprise web interface showing the configuration for an alert named "final project football (events for chelsea)". The interface has a dark theme. At the top, there's a navigation bar with "splunk-enterprise" and "Apps" on the left, and user roles like "Administrator", "Messages", "Settings", "Activity", "Help", and a "Find" search bar on the right. Below the navigation bar is a sub-navigation bar with "Search", "Analytics", "Datasets", "Reports", "Alerts", and "Dashboards". The main content area shows the alert configuration details. On the left, it lists: "Enabled: Yes. [Disable](#)", "App:search", "Permissions: Private. Owned by mahmoud. [Edit](#)", "Modified: Dec 24, 2024 6:50:06 AM", and "Alert Type: Scheduled. Weekly, Monday at 6:00. [Edit](#)". On the right, it shows: "Trigger Condition: .. Number of Results is > 0. [Edit](#)" and "Actions: 1 Action [Edit](#)", with a sub-action "Send email" indicated by an envelope icon. At the bottom, there's a message: "There are no fired events for this alert." with an information icon.

final project football (draw matches)

draw matches

Enabled: Yes. [Disable](#)

App:search

Permissions:Private. Owned by mahmoud. [Edit](#)

Modified:Dec 24, 2024 6:53:43 AM

Alert Type:Scheduled. Weekly, Monday at 6:00. [Edit](#)

Trigger Condition: ...Number of Results is > 0. [Edit](#)

Actions:1 Action



Output results to lookup

[Edit](#)

final project football (events after 80)

events after 80

Enabled: Yes. [Disable](#)

App: search

Permissions:Private. Owned by mahmoud. [Edit](#)

Modified:Dec 24, 2024 6:48:20 AM

Alert Type: Scheduled. Weekly, Monday at 6:00. [Edit](#)

Trigger Condition: Number of Results is > 0. [Edit](#)

Actions: 1 Action



Log Event

[Edit](#)

A screenshot of the Splunk Enterprise web interface showing the configuration for an alert named "final project football (events after 80)". The interface has a dark theme. At the top, there's a navigation bar with "splunk-enterprise" and "Apps". Below it, a secondary navigation bar lists "Search", "Analytics", "Datasets", "Reports", "Alerts", and "Dashboards". The main content area shows the alert title "final project football (events after 80)" with an "Edit" button. Below the title, the alert is described as "events after 80". Configuration details are listed in two columns: "Enabled: Yes. Disable", "App: search", "Permissions: Private. Owned by mahmoud. Edit", "Modified: Dec 24, 2024 6:48:20 AM", and "Alert Type: Scheduled. Weekly, Monday at 6:00. Edit" on the left; and "Trigger Condition: .. Number of Results is > 0. Edit" and "Actions: 1 Action Edit" (with a dropdown showing "Log Event") on the right. At the bottom, a message states "There are no fired events for this alert."

final project football (goal before 5)

goal before 5

Enabled: Yes. [Disable](#)

App: search

Permissions:Private. Owned by mahmoud. [Edit](#)

Modified:Dec 24, 2024 6:57:37 AM

Alert Type: Scheduled. Weekly, Monday at 6:00. [Edit](#)

Trigger Condition: ...Number of Results is > 0. [Edit](#)

Actions:5 Actions



Add to Triggered Alerts



Send email



Log Event



Output results to lookup



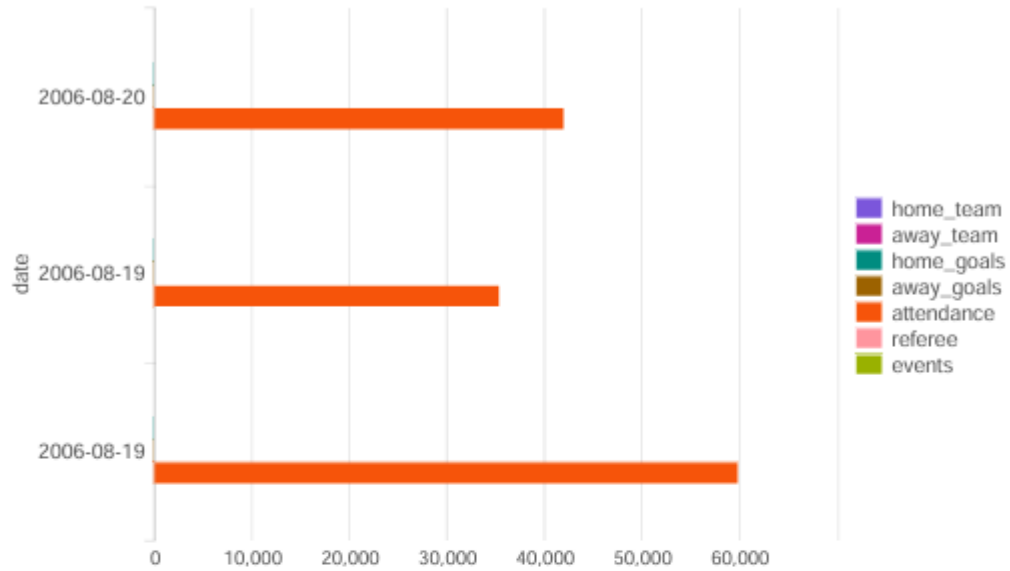
Run a script

[Edit](#)

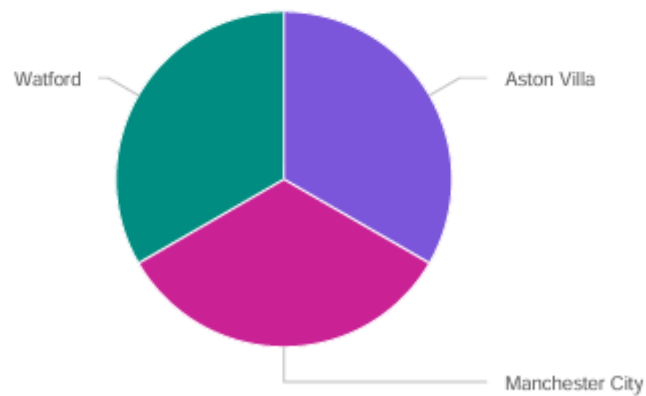
There are no fired events for this alert.

The screenshot shows the Splunk Enterprise web interface. At the top, there's a navigation bar with 'splunk-enterprise' and 'Apps'. Below it, a secondary navigation bar includes 'Search', 'Analytics', 'Datasets', 'Reports', 'Alerts', and 'Dashboards'. The main content area displays the configuration for an alert titled 'final project football (goal before 5)'. The alert is enabled and owned by 'mahmoud'. Its trigger condition is 'Number of Results is > 0'. It has five actions: 'Add to Triggered Alerts', 'Send email', 'Log Event', 'Output results to lookup', and 'Run a script'. At the bottom, a message states 'There are no fired events for this alert.'

show all data



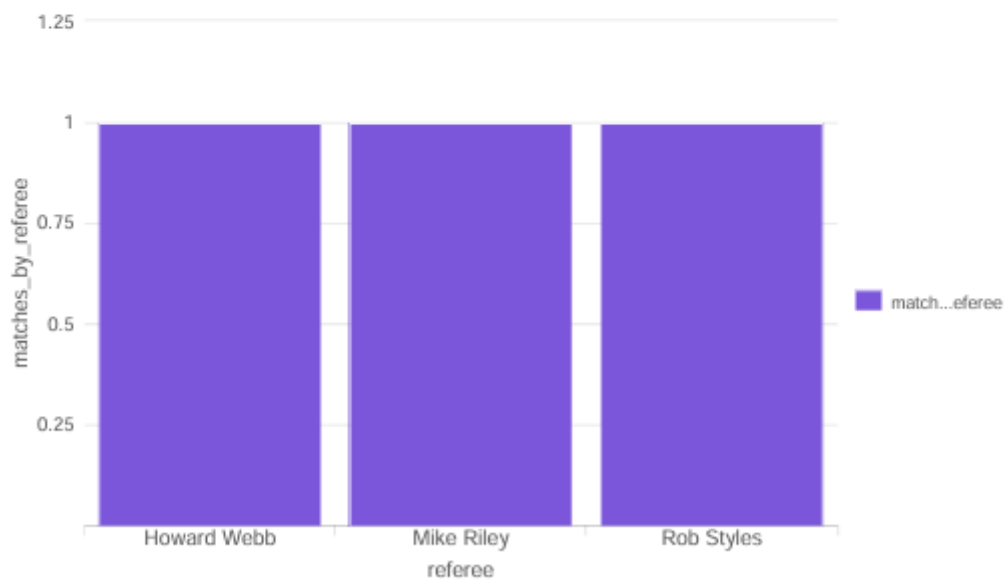
total goals for every team



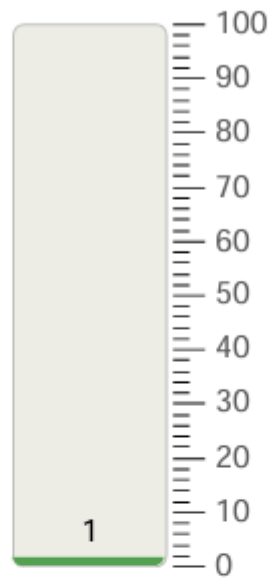
avg attendance in matches



matches by referee



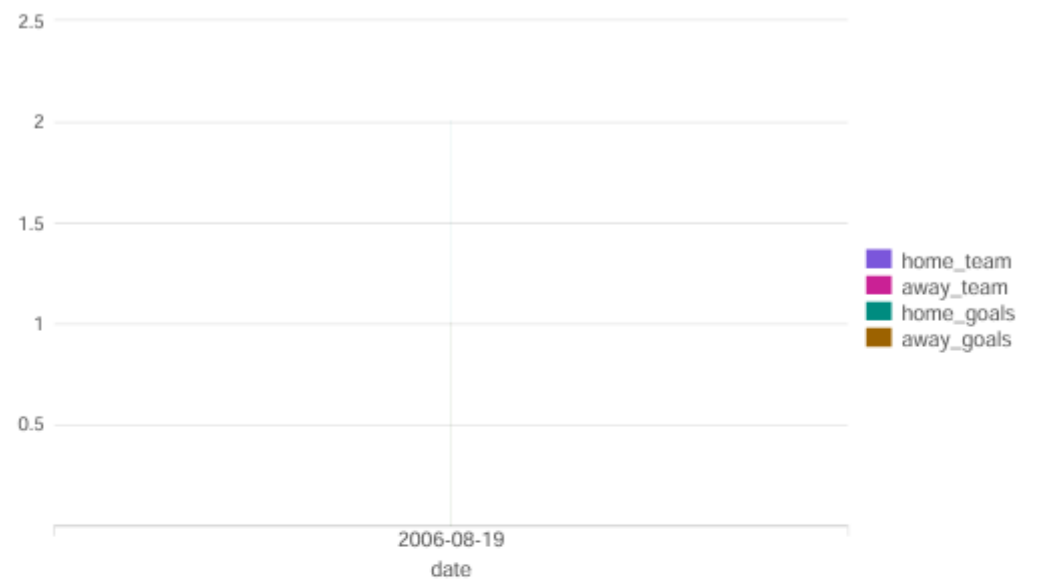
draw matches



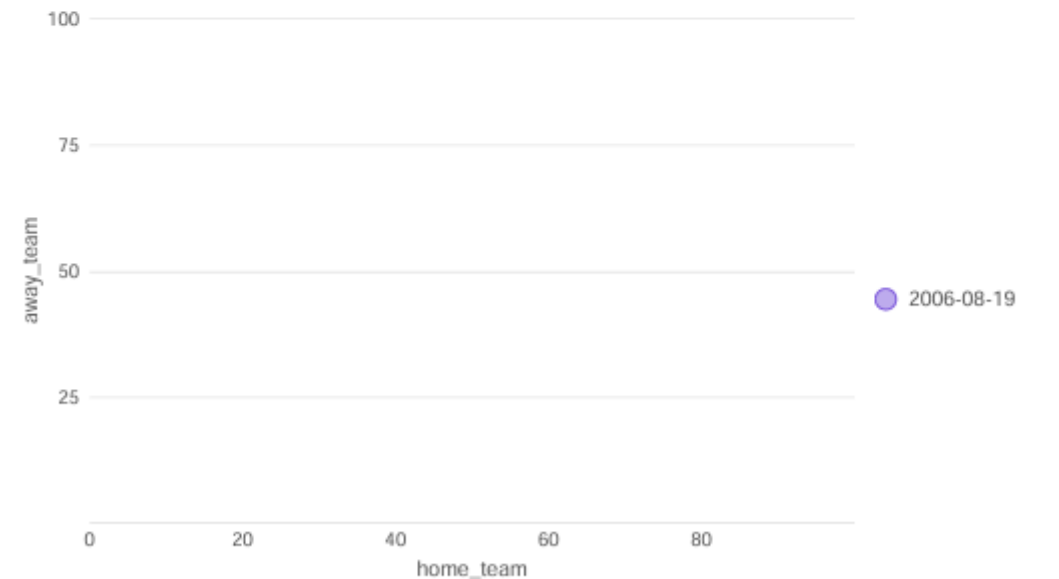
avg goals every match

3

matches end goal difference 1



matches by referee "howard webb"



attendance >40000

